JP00/4372

PCT/JP00/07473
25.10.00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

EW

出願年月日
Date of Application: １９９９年１０月２５日

出願番号
Application Number: 平成１１年特許願第３０３１４２号

出願人
Applicant (s): ソニー株式会社

09857218

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２０００年 ９月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０７５３４７

【書類名】　特許願

【整理番号】　9900793602

【提出日】　平成11年10月25日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石黒　隆二

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　河上　達

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　田辺　充

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　江面　裕一

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　佐藤　一郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　海老原　宗毅

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ提供システム及びコンテンツ提供方法

【特許請求の範囲】

【請求項１】　コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、

上記データ処理装置は、

上記再生プログラムがインストールされた後に、第１のマスター鍵及び第１の認証鍵が上記再生プログラムに提供され、上記第１のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第１の認証鍵及び第１のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第１のマスター鍵とは異なる第２のマスター鍵及び上記第１の認証鍵とは異なる第２の認証鍵がネットワークを介して提供され、この提供された第２のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第２の認証鍵及び第２のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供システム。

【請求項２】　上記可搬再生装置は、第１から第ｉ（ｉは２以上の整数）世代まで世代更新されていく第１から第ｉの認証鍵、及び、第１から第ｉ（ｉは２以上の整数）世代まで世代更新されていく第１から第ｉのマスター鍵を保持しており、

上記再生プログラムは、第２から第ｉ（ｉは２以上の整数）まで世代更新されていく第２から第ｉの認証鍵、及び、第２から第ｉ（ｉは２以上の整数）まで世代更新されていく第２から第ｉのマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求項１記載のコンテンツ提供システム。

【請求項３】　上記可搬再生装置は、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項２記載のコンテンツ提供システム。

【請求項４】　上記再生プログラムは、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項２記載のコンテンツ提供システム。

【請求項５】　上記コンテンツサーバは、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが用いている認証鍵の世代更新をすること

を特徴とする請求項２記載のコンテンツ提供システム。

【請求項６】　コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、

上記再生プログラムをインストールした後に、第１のマスター鍵及び第１の認証鍵が上記再生プログラムに提供され、上記第１のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第１の認証鍵及び第１のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、

上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第１のマスター鍵とは異なる第２

のマスター鍵及び上記第１の認証鍵とは異なる第２の認証鍵がネットワークを介して提供され、この提供された第２のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第２の認証鍵及び第２のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うこと

を特徴とするコンテンツ提供方法。

【請求項７】　上記可搬再生装置が、第１から第ｉ（ｉは２以上の整数）世代まで世代更新されていく第１から第ｉの認証鍵、及び、第１から第ｉ（ｉは２以上の整数）世代まで世代更新されていく第１から第ｉのマスター鍵を保持しており、

上記再生プログラムは、第２から第ｉ（ｉは２以上の整数）まで世代更新されていく第２から第ｉの認証鍵、及び、第２から第ｉ（ｉは２以上の整数）まで世代更新されていく第２から第ｉのマスター鍵がネットワークを介して提供され、

上記可搬再生装置と上記再生プログラムとは、同一世代の認証鍵を用いて相互認証を行うこと

を特徴とする請求項６記載のコンテンツ提供方法。

【請求項８】　上記可搬再生装置が、上記再生プログラムと認証を行った際に、この再生プログラムが用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記再生プログラムが用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項７記載のコンテンツ提供方法。

【請求項９】　上記再生プログラムが、上記可搬再生装置と認証を行った際に、上記可搬再生装置が用いている世代よりも古い世代の認証鍵及びマスター鍵を用いている場合には、上記コンテンツサーバに鍵要求をして、上記可搬再生装置が用いている世代まで自己の認証鍵及びマスター鍵の世代を更新すること

を特徴とする請求項７記載のコンテンツ提供方法。

【請求項１０】　上記コンテンツサーバが、上記再生プログラムからアクセスされた際に、上記再生プログラムが用いている認証鍵の世代よりも新しい世代の認証鍵及びマスター鍵を上記再生プログラムに提供して、上記再生プログラムが

用いている認証鍵の世代更新をすること

を特徴とする請求項７記載のコンテンツ提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

半導体メモリやメモリカード等を記憶媒体とした可搬再生装置にコンテンツデータを提供するコンテンツ提供システム及びコンテンツ提供方法に関するものである。

【０００２】

【従来の技術】

近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオンライン配信が実用化され始めた。

【０００３】

このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Ｗｅｂ上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するＷｅｂ等にアクセスをして、所望の音楽コンテンツをダウンロードする。ユーザは、取得した音楽コンテンツを、例えば、パーソナルコンピュータ内のプレーヤアプリケーションにより再生したり、また、このパーソナルコンピュータと接続可能なポータブルデバイス等により再生する。

【０００４】

ここで、コンテンツ提供業者は、そのコンテンツの著作権を管理しなければならない。そのため、コンテンツ配信業者は、インターネットを介してＷｅｂ上にアクセスしてきたユーザをＩＤ情報や暗証番号等で認識し、正当なユーザに対してのみに暗号化した音楽コンテンツを配信する。そして、その音楽コンテンツは、ユーザからは自由に参照できないような暗号鍵により鍵管理がされた状態で、パーソナルコンピュータ内のハードディスクに格納される。また、パーソナルコンピュータ内に格納された音楽コンテンツをポータブルデバイスに転送する場合

には、プレーヤアプリケーションとポータブルデバイスとの間で認証処理を行った後に、ポータブルデバイスが有する記憶媒体に音楽コンテンツが格納される。

【０００５】

【発明が解決しようとする課題】

ところで、一般に、ポータブルデバイスやには、ネットワークから配信された音楽コンテンツのみならず、例えばＣＤ等のメディアから音楽コンテンツをコピーすることもできる。

【０００６】

ところが、従来、ポータブルデバイスとパーソナルコンピュータと間の認証の方式は、ＣＤ等のメディアからコピーされた音楽コンテンツのみを扱うプレーヤアプリケーションであろうが、ネットワークからダウンロードした音楽コンテンツを扱うプレーヤアプリケーションであろうが、特に区別がされず行われていた。

【０００７】

そのため、例えば、なんらかの悪意を有する者により、ポータブルデバイスとパーソナルコンピュータとの認証鍵が破られた場合、ＣＤ等のメディアからコピーされた音楽コンテンツと、ネットワークを介して配信した音楽コンテンツとの両者ともに不正にコピーがされてしまう。

【０００８】

特に、ＣＤ等のメディアの場合は、一般にメディアが販売された時に課金が終了している場合が主であるが、ネットワークを介して配信された音楽コンテンツは、例えば、再生をした回数や複製をした回数等に応じて課金等がされる場合があり、より強固な鍵管理が望まれる。

【０００９】

本発明は、ネットワークを介して配信されたコンテンツデータの安全性を高めることができるコンテンツ提供システム及びコンテンツ提供方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明にかかるコンテンツ提供システムは、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとからなるコンテンツ提供システムにおいて、上記データ処理装置は、上記再生プログラムがインストールされた後に、第１のマスター鍵及び第１の認証鍵が上記再生プログラムに提供され、上記第１のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第１の認証鍵及び第１のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムが上記コンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第１のマスター鍵とは異なる第２のマスター鍵及び上記第１の認証鍵とは異なる第２の認証鍵がネットワークを介して提供され、この提供された第２のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第２の認証鍵及び第２のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

【００１１】

コンテンツ提供システムでは、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第２の認証鍵及び第２のマスター鍵は、ネットワークを介して再生プログラムに提供され、第１の認証鍵及び第１のマスター鍵と異なる鍵となっている。

【００１２】

本発明にかかるコンテンツ提供方法は、コンテンツデータを再生する再生プログラムを有するデータ処理装置と、上記データ処理装置から提供されたコンテンツデータを記憶媒体に格納して再生する可搬再生装置とによりユーザにコンテンツデータを提供するコンテンツサーバとからなるコンテンツ提供方法において、上記再生プログラムをインストールした後に、第１のマスター鍵及び第１の認証鍵が上記再生プログラムに提供され、上記第１のマスター鍵を用いて当該装置に接続された外部記憶媒体に格納されたコンテンツデータを取得して保存し、上記再生プログラムがこの提供された第１の認証鍵及び第１のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行い、上記再生プログラムがコンテンツサーバから配信されたコンテンツデータの送受信を上記可搬再生装置と行う場合には、上記第１のマスター鍵とは異なる第２のマスター鍵及び上記第１の認証鍵とは異なる第２の認証鍵がネットワークを介して提供され、この提供された第２のマスター鍵を用いて上記コンテンツサーバから提供されたコンテンツデータを取得して保存し、この提供された第２の認証鍵及び第２のマスター鍵を用いて上記可搬再生装置との認証を行ってコンテンツデータの送受信を行うことを特徴とする。

【００１３】

このコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第２の認証鍵及び第２のマスター鍵は、ネットワークを介して再生プログラムに提供され、第１の認証鍵及び第１のマスター鍵と異なる鍵となっている。

【００１４】

【発明の実施の形態】

（１）音楽コンテンツ配信システムの全体構成

図１に本発明を適用した実施の形態の音楽コンテンツ配信システム１のシステム構成を示す。

【００１５】

本発明の実施の形態の音楽コンテンツ配信システム１は、この図１に示すように、インターネット等のネットワーク２を介して音楽コンテンツの提供等をする複数のＥＭＤ（Electrical Music Distribution）サーバと、各ＥＭＤサーバから上記ネットワーク２を介して音楽コンテンツの配信を受けるパーソナルコンピュータ（以下、単にパソコンと略して称する。）３と、このパソコン３とＵＳＢ（Universal Serial Bus）等のインターフェース４により接続されこのパソコン３から音楽コンテンツが転送されて再生を行う携帯型の音楽再生機器である複数のポータブルデバイス（ＰＤ）とを備える構成となっている。

【００１６】

音楽コンテンツ配信システム１を構成している複数のＥＭＤサーバには、例えば音楽提供会社Ａから提供される音楽コンテンツを配信するＥＭＤサーバ（Ａ）５と、例えば音楽提供会社Ｂから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｂ）６と、例えば音楽提供会社Ｘから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｘ）７とがある。各ＥＭＤサーバ５，６，７は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパソコン３にネットワーク２を介して提供を行っている。また、各ＥＭＤサーバ５，６，７では、音楽コンテンツの暗号化方式、利用条件（Usage Rule）情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等は、各社独自の方式が採用されており、各ＥＭＤサーバ５，６，７では、それぞれ異なる方式により音楽コンテンツを配信している。

【００１７】

パソコン３には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、ＥＭＤサーバ（Ａ）から音楽コンテンツの購入や管理を行う購入用アプリケーション（Ａ）１１と、ＥＭＤサーバ（Ｂ）から音楽コンテンツの購入や管理を行う購入用アプリケーション（Ｂ）１２と、ＥＭＤサーバ（Ａ）５から購入した音楽コンテンツの再生を行うデバイスドライバ（Ａ）１３と

、ＥＭＤサーバ（Ｂ）６から購入した音楽コンテンツの再生を行うデバイスドライバ（Ｂ）１４とがインストールされている。また、パソコン３には、ハードディスク１９内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット（Ｘ）１５がインストールされている。この包括管理ユニット（Ｘ）１５は、さらに、ＥＭＤ用受信インターフェース１６，ＥＭＤ用送信インターフェース１７，ＰＤ用ドライバ１８により構成されている。

【００１８】

ポータブルデバイス（Ａ）８は音楽提供会社Ａに対応した専用の装置であり、ポータブルデバイス（Ｂ）９は音楽提供会社Ｂに対応した専用の装置であり、ポータブルデバイス（Ｘ）１０は音楽提供会社Ｘに対応した専用の装置である。

【００１９】

各ポータブルデバイス８，９，１０は、音楽コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なＩＣメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス８，９，１０は、ＵＳＢ等の物理的なインターフェース４を介して各デバイスドライバ１３，１４及びＰＤドライバ１８と接続され、音楽コンテンツが転送される。このとき、音楽コンテンツは、暗号化及び圧縮された状態で提供され、利用条件情報も付加されている。

【００２０】

各ポータブルデバイス８，９，１０は、各デバイスドライバ１３，１４及びＰＤドライバ１８から転送された音楽コンテンツを、各音楽コンテンツに付加された利用条件情報とともに、メモリカード等の記憶媒体内に暗号化して格納する。そして、各ポータブルデバイス８，９，１０は、通常、パソコン３との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化した音楽コンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス８，９，１０は、各音楽コンテンツに付加されている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、音楽コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。なお、メモリカード内に格納した音楽コンテンツは、各デバイスドライバ１３，１４及び包括管理ユニット

（Ｘ）１５やポータブルデバイス８，９，１０独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっている。

【００２１】

購入用アプリケーション（Ａ）１１は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この購入用アプリケーション（Ａ）１１は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。具体的には、購入用アプリケーション（Ａ）１１は、ＥＭＤサーバ（Ａ）５に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、購入用アプリケーション（Ａ）１１は、ＥＭＤサーバと接続した際の認証処理、ポータブルデバイスと接続した際の認証処理、ハードディスク１９に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。購入用アプリケーション（Ａ）１１は、例えば、ＥＭＤサーバからダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ハードディスク１９に格納する。なお、暗号化処理の方式は、各購入用アプリケーションでそれぞれ独自の方式を採用している。そのため、パソコン３内の同一のハードディスク１９に格納されている音楽コンテンツであっても、専用の購入用アプリケーションでなければ、他の購入用アプリケーションでは暗号を解読することができないようになっている。

【００２２】

また、購入用アプリケーション（Ａ）１１は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、購入用アプリケーション（Ａ）１１は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【００２３】

また、購入用アプリケーション（Ａ）１１は、自己がハードディスク１９上に

管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（Ｘ）１５のＥＭＤ用受信インターフェース１６に送信する。

【００２４】

購入用アプリケーション（Ｂ）１２は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この購入用アプリケーション（Ｂ）１２は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。具体的には、購入用アプリケーション（Ｂ）１２は、ＥＭＤサーバ（Ｂ）６に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、購入用アプリケーション（Ｂ）１２は、ＥＭＤサーバと接続した際の認証処理、ポータブルデバイスと接続した際の認証処理、ハードディスク１９に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。購入用アプリケーション（Ｂ）１２は、例えば、ＥＭＤサーバからダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ハードディスク１９に格納する。

【００２５】

また、購入用アプリケーション（Ｂ）１２は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、購入用アプリケーション（Ｂ）１２は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【００２６】

また、購入用アプリケーション（Ｂ）１２は、包括管理ユニット（Ｘ）１５のＥＭＤ用受信インターフェース１６との間で、自己がハードディスク１９上に管理している音楽コンテンツ及び利用条件情報を、相互に転送を行う。

【００２７】

デバイスドライバ（Ａ）１３は、音楽コンテンツの再生や、ポータブルデバイス（Ａ）８への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ａ）１３は、購入用アプリケーション（Ａ）１１によ

り管理されている音楽コンテンツや包括管理ユニット（Ｘ）１５により管理されている音楽コンテンツの再生を行い、また、ポータブルデバイス（Ａ）８にこれらの音楽コンテンツを転送する。また、デバイスドライバ（Ａ）１３は、音楽コンテンツの再生時においては、音楽コンテンツの伸張処理も行う。圧縮伸張処理の方式は、各デバイスドライバでそれぞれ独自の方式を採用している。

【００２８】

デバイスドライバ（Ｂ）１４は、音楽コンテンツの再生や、ポータブルデバイス（Ｂ）９への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ｂ）１４は、購入用アプリケーション（Ｂ）１２により管理されている音楽コンテンツや包括管理ユニット（Ｘ）１５により管理されている音楽コンテンツの再生を行い、また、ポータブルデバイス（Ｂ）９にこれらの音楽コンテンツを転送する。また、デバイスドライバ（Ｂ）１４は、音楽コンテンツの再生時においては、音楽コンテンツの伸張処理も行う。

【００２９】

包括管理ユニット（Ｘ）１５は、ＥＭＤサーバ（Ｘ）７から音楽コンテンツの提供を受ける音楽提供会社Ｘ専用のアプリケーションソフトウェアであるとともに、デバイスドライバ（Ａ）１３及びデバイスドライバ（Ｂ）１４や、購入用アプリケーション（Ａ）１１及び購入用アプリケーション１２との間で音楽コンテンツ及び利用条件情報の転送を行って、パソコン３内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス（Ｘ）１０に転送することができる。

【００３０】

ＰＤ用ドライバ１８は、ポータブルデバイス（Ｘ）１０との接続用のインターフェースモジュールで、このポータブルデバイス（Ｘ）１０との間における認証処理や暗号化処理を行う。また、ＰＤ用ドライバ１８は、他のポータブルデバイス８，９に音楽コンテンツ等を転送する場合には、デバイスドライバ（Ａ）１３やデバイスドライバ（Ｂ）１４を介して音楽コンテンツ及び利用条件情報を転送する。

【００３１】

ＥＭＤ用受信インターフェース１６は、購入用アプリケーション（Ａ）１１からの音楽コンテンツ及び利用条件情報の受信、ＥＭＤサーバ（Ｘ）７からネットワーク２を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、オーディオプレーヤ（Ｂ）１２との間での音楽コンテンツ及び利用条件情報の送受信を行う。

【００３２】

ＥＭＤ用受信インターフェース１６は、購入用アプリケーション（Ａ）１１から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、購入用アプリケーション（Ａ）１１が用いている方式から、包括管理ユニット（Ｘ）１５が用いている方式に変換される。ここで包括管理ユニット（Ｘ）１５が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、ＥＭＤ用受信インターフェース１６は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、購入用アプリケーション（Ｂ）１２に送信したり、また、ＰＤ用ドライバ１８を介してデバイスドライバ（Ａ）１３やデバイスドライバ（Ｂ）１４に送信する。また、ＥＭＤ用受信インターフェース１６は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、ＰＤドライバ１８を介して、ポータブルデバイス（Ｘ）１０に送信する。

【００３３】

また、ＥＭＤ用受信インターフェース１６は、購入用アプリケーション（Ｂ）１２との間で、音楽コンテンツ及び利用条件情報の送受信を行う。ここで、購入用アプリケーション（Ｂ）１２は、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、圧縮方式が、上記統一転送プロトコルと同一となっている。したがって、この間では、利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換は行われない。

【００３４】

また、ＥＭＤ用受信インターフェース１６は、購入用アプリケーション（Ａ）１１により管理されている音楽コンテンツ、ＥＭＤサーバ（Ｘ）７からダウンロードした音楽コンテンツを、受信する。ここで、ＥＭＤサーバ（Ｘ）７は、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、圧縮方式が、上記統一転送プロトコルと同一となっている。したがって、この間では、利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換は行われない。

【００３５】

このようなＥＭＤ用受信インターフェース１６は、ＥＭＤサーバ（Ｘ）７から音楽コンテンツ及び利用条件情報を受信して購入用アプリケーション１２に転送し、また、購入用アプリケーション（Ａ）１１から暗号化方式、利用条件情報のフォーマット、圧縮方式が異なる音楽コンテンツを受信してそれを購入用アプリケーション（Ｂ）１２に転送する。そして、購入用アプリケーション１２は、ＥＭＤサーバ（Ａ）５、ＥＭＤサーバ（Ｂ）６、ＥＭＤサーバ（Ｘ）からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行う。

【００３６】

また、ＥＭＤ用受信インターフェース１６は、音楽コンテンツの複製（コピー）、移動（ムーブ）、チェックイン、チェックアウトの機能を有している。

【００３７】

ＥＭＤ用受信インターフェース１６は、ユーザからの複製命令、移動命令に従い、例えば、購入用アプリケーション（Ａ）１１に格納されている音楽コンテンツを、購入用アプリケーション（Ｂ）１２に複製や移動する処理を行う。この際に、ＥＭＤ用受信インターフェース１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

【００３８】

また、ユーザからのチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス８，９，１０に格納されている音楽コンテンツを、

購入用アプリケーション（Ｂ）１２に複製や移動する処理を行う。この際に、ＥＭＤ用受信インターフェース１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【００３９】

また、ユーザからのチェックアウト命令に従い、購入用アプリケーション（Ａ）１１や購入用アプリケーション（Ｂ）１２に格納されている音楽コンテンツを、ポータブルデバイス１０に移動する処理を行う。この際に、ＥＭＤ用受信インターフェース１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【００４０】

また、包括管理ユニット（Ｘ）１５では、図２に示すように、アプリケーション層の下位レイヤに統一転送プロトコルを設けて、このレイヤにおいて他の購入用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット（Ｘ）１５は、この統一転送プロトコルの更に下位レイヤをｈｔｔｐとして、ＥＭＤサーバ（Ｘ）７とのデータ送受信を行っている。

【００４１】

以上のような構成の音楽コンテンツ配信システム１では、ＥＭＤサーバ（Ａ）５から配信された音楽コンテンツを、デバイスドライバ（Ａ）１３及びポータブルデバイス（Ａ）８が取得し、再生を行うようになっている。また、ＥＭＤサーバ（Ｂ）６から配信された音楽コンテンツを、デバイスドライバ（Ｂ）１４及びポータブルデバイス（Ａ）９が取得し、再生を行うようになっている。また、ＥＭＤサーバ（Ｘ）７、ＥＭＤサーバ（Ａ）及びＥＭＤサーバ（Ｂ）から配信された音楽コンテンツを、ポータブルデバイス（Ｘ）１０が再生を行うようになっている。

【００４２】

以上のように音楽コンテンツ配信システム１では、包括管理ユニット（Ｘ）１５を中心として、各購入用アプリケーション及びデバイスドライバの間で、転送

する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの相互転送が行われる。そのため、例えば、購入用アプリケーション（Ａ）１１によりＥＭＤサーバ（Ａ）５からダウンロードした音楽コンテンツを、包括管理ユニット（Ｘ）１５を介して購入用アプリケーション（Ｂ）１２に転送することができ、このため、例えば音楽提供会社Ａからのみ提供されるアーチストの音楽コンテンツを、デバイスドライバ（Ｂ）１４やポータブルデバイス（Ａ）９やポータブルデバイス（Ｘ）１０により再生することができる。すなわち、この音楽コンテンツ配信システム１では、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パソコン３のハードディスク内に格納されている様々な方式の音楽コンテンツを、任意の１つのオーディオプレーヤやポータブルデバイスにより再生を行うことができる。特に、音楽コンテンツ配信システム１では、相互転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

【００４３】

すなわち、音楽コンテンツ配信システム１では、音楽コンテンツの再生や制御を行うオーディオプレーヤ間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システム１では、複数のオーディオプレーヤが存在してもパソコン３内の例えばハードディスク１９に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。また、音楽コンテンツとともに利用条件情報も転送するので、１つの音楽コンテンツに対して利用条件が重複したりすることがなく、音楽コンテンツの著作権も確実に保護することができる。

【００４４】

（２）利用条件情報

（一般的に用いられる利用条件情報の説明）

購入用アプリケーション（Ａ）１１に用いられる利用条件情報のフォーマットの一例について説明をする。

【００４５】

購入用アプリケーション（Ａ）１１では、例えば、図３（ａ）に示すような表形式で記述された利用条件情報が用いられている。

【００４６】

表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日（ｆｒｏｍ）、再生終了日（ｔｏ）、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）等が記述される。このような利用条件情報は、図３（ｂ）に示すように各音楽コンテンツに付加された状態で、ＥＭＤサーバ（Ａ）５から配信される。購入用アプリケーション（Ａ）１１は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日（ｆｒｏｍ）が９９年１０月２５日、再生終了日（ｔｏ）が９９年１１月２４日、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）がｙｅｓ／１０円と記述されているとする。この場合、その音楽コンテンツは、９９年１０月２５日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、９９年１１月２４日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、１回の再生の度に１０円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として保管しておき、そのログ情報をＥＭＤサーバ（Ａ）５にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

【００４７】

（包括管理ユニット（Ｘ）１５が用いている利用条件情報の説明）

包括管理ユニット（Ｘ）１５が用いている利用条件情報について説明する。以下説明をする利用条件情報は、ＥＭＤサーバ（Ｘ）７からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット（Ｘ）１５がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、購入用アプリケーション（Ａ）１１と包括管理ユニット（Ｘ）１５との間、及び、購入用ア

プリケーション（Ａ）１１と包括管理ユニット（Ｘ）１５との間で、音楽コンテンツの相互転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

【００４８】

統一利用条件情報は、図４に示すように、インデックスファイル３１、オートマトンファイル３２と、パラメータファイル３３と、履歴ファイル３４とから構成される。各ファイルは、ＸＭＬ言語で記述されている。

【００４９】

インデックスファイル３１には、各ファイルのリファレンス情報等が記述されている。

【００５０】

オートマトンファイル３２には、図５に示すように、利用条件がオートマトンで記述されたオートマトン記述部４１と、コンテンツ鍵による認証コード（ＭＡＣ:Message Authentication Code）４２、コンテンツ提供者の署名（Ｓｉｇ）４３、この署名を検証するための認証書（Ｃｅｒｔ）４４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれK^{-1}_E, K^{1}_Eとする。

【００５１】

オートマトン記述部４１は、tuple列で記述されたExtended State Machineにより音楽コンテンツの動作状態が記述される。

【００５２】

具体的には、オートマトン記述部４１では、現在の音楽コンテンツの動作状態の集合をＱとし、音楽コンテンツのイベントを表す入力シンボルの集合をΣとし、状態遷移した後の音楽コンテンツの動作状態の集合をＱ′を以下のように表す。

【００５３】

$Q' = \{d \mid d = \delta(q, \alpha) \mid q \quad Q, \alpha \quad Q, \delta : Q \times \Sigma \rightarrow Q\}$

そして、以上のＱ，Σ，Ｑ′に基づき、各tupleを

$\{\langle q, \alpha, d \rangle \mid q, d \quad Q, \alpha \quad \Sigma\}$

として表す。

【００５４】

ここで、Σには、再生（Play），複製（copy），支払い金額（pay Y），再生開始可能日時（from YMD），再生終了日時（to YMD），使用可能日数（in Ddays），ヌルイベント（ε）といったイベントが、以下のように記述される。

【００５５】

Σ＝｛Play,copy,pay Y,from YMD,to YMD,in Ddays,ε｝

例えば、オートマトン記述部４１には、図６に示すような音楽コンテンツの動作遷移を示すオートマトンを、図７に示すようなtuple列にして記述する。

【００５６】

また、オートマトン記述部４１は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作a_0と動作a_1との並列合成は、tuple列で以下のように表される。

【００５７】

$\langle q_0,\ \alpha,\ a_0 \cdot\ q_0\rangle$

$\langle q_0,\ \alpha,\ a_1 \cdot\ q_0\rangle$

また、オートマトン記述部４１には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tupleで以下のように表される。

【００５８】

$\langle q_0,\ \alpha,\ q_1;\ action\rangle$

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、ＩＤとスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム（ａ）の買い取りの値段を表す変数をｎとし、ａ．ｎ：＝１０００のように記述する。このように変数に対するアクションが記述されたオートマトン記述部４１の一例を以下に示す。

【００５９】

$\langle q_0,\ pay100,\ q_1,\ a.\ n:=a.\ n-100\rangle$　　・・・（1）

$\langle q_0,\ pay\ (a.\ n),\ q_1,\ a.\ n:=0\rangle$　　・・・（2）

$\langle q_1, play, q_2 \rangle$ ・・・（３）

この例は、１つの音楽コンテンツの買い取り値段〔式（１）〕が、アルバム買い取り〔式（２）〕の値段に影響を及ぼすことを示している。

【００６０】

以上のようなオートマトン記述部４１は、図８に示すように、エントリーＩＤ４５と、コンテンツＩＤ４６と、バージョン情報４７と、変数情報４８と、tuple４９列とから構成される。

【００６１】

以上のように記述フォーマットが定められたオートマトン記述部４１の具体例を図９～図１２に示す。なお、以下の図９～図１２の記述で用いられているイベントとコマンドとを図１３に示す。

【００６２】

図９は、音楽コンテンツが１９９９年９月１日から再生が可能であることを示すＸＭＬ言語によるオートマトン記述部４１の記述例である。

【００６３】

図１０は、音楽コンテンツが１９９９年１０月３１日まで再生が可能であることを示すＸＭＬ言語によるオートマトン記述部４１の記述例である。

【００６４】

図１１は、音楽コンテンツの再生回数を１６回に制限することを示すＸＭＬ言語によるオートマトン記述部４１の記述例である。

【００６５】

図１２は、音楽コンテンツの再生可能期間が１９９９年９月１日から１９９９年１０月３１日までであって、且つ、その再生可能回数が１６回であることを示すＸＭＬ言語によるオートマトン記述部４１の記述例である。

【００６６】

図１３は、再生動作（play）、複製動作（copy）、再生権購入（pay-for-play）、複製権購入（pay-for-copy）、アルバム再生権購入（pay-for-album-play）、アルバム複製権購入（pay-for-album-copy）、使用可能開始日（from）、使用終了日（to）、ヌル動作（null）がイベントとして設定されている例である。

【００６７】

つぎに、パラメータファイル３３には、図１４に示すように、パラメータ記述部５１、コンテンツ鍵による認証コード５２、コンテンツ提供者の署名５３、この署名を検証するための認証書５４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれ$K^{-1}{}_E$，$K^{1}{}_E$とする。

【００６８】

また、パラメータファイル３３は、上記オートマトンファイル３２を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル３３は、図１５に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティＩＤ５５が付加される。ここで、K'_Cは、二次提供者のコンテンツ鍵で、$K'_C = H(K_C, \mathrm{EntityID})$となる。二次提供者のコンテンツ鍵$K'_C$は、一次提供者のコンテンツ鍵$K_C$から作成される。一次提供者と二次提供者とは、その認証書により区別される。

【００６９】

パラメータファイル３３を検証する方法としては、コンテンツ鍵が得られていればＭＡＣにより行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

【００７０】

ＭＡＣにより検証するプロトコルは以下のようになる。コンテンツの一次提供者をＳ、二次提供者をＡ、端末をＢとする。

【００７１】

$S \rightarrow A$ ： $K'_C = H(K_C, ID_A)$

$S \rightarrow B$ ： $X = E_{Ks}(K_C)^1$

$A \rightarrow B$ ： ID_A, Parameters, $M = MACK'_C$ (Parameters)

B ： $M \equiv MAC_{K'_c}$ (Parameters) ？

このパラメータ記述部５１には、上記オートマトンファイル３１のオートマトン部４１に記述された値の変更のための関数の係数が記述される。例えば、図７

に示した例において、オートマトン部４１では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

【００７２】

$\langle q_0, pay(f_1(10)), q_1\rangle$

$\langle q_1, pay(f_2(10)\times n), q_2\rangle$

この場合、上記関数f_1及びf_2を、例えば、以下のように定める。

【００７３】

$f_1(n)=0.9n$

$f_2(n)=90+0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル３３を書き換えて、価格を変更することができる。

【００７４】

以上のようなパラメータ記述部５１は、図１６に示すように、エントリーＩＤ５６と、コンテンツＩＤ５７と、係数情報５８とから構成される。

【００７５】

履歴ファイル３４は、オートマトン記述部４１に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。上記オートマトン記述４１のｔｕｐｌｅ内のステータスと変数を記録する。例えば、上述した図７に例において、２回再生を行った場合には、

$\langle q_0, q_1, q_0, q_1\rangle$

となり、これにより以下のような動作の軌跡を得ることができる。

【００７６】

〈ｐａｙ１０，ｐｌａｙ，ｐａｙ１０，ｐｌａｙ〉

これを集計して、例えば、包括管理ユニット（Ｘ）１５にアップロード等すれば、ユーザの支払い金額を計算することができる。

【００７７】

以上のように音楽コンテンツ配信システム１では、オートマトンにより利用条件を表現した統一利用条件情報を用いているので、コンテンツの利用条件の記載

の自由度を高めることができる。

【００７８】

（３）破壊された音楽コンテンツ等のリストア及び再ダウンロード

つぎに、包括管理ユニット（Ｘ）１５による音楽コンテンツのバックアップについて説明をする。

【００７９】

まず、包括管理ユニット（Ｘ）１５の音楽コンテンツの鍵管理方法について、図１７を用いて説明する。

【００８０】

包括管理ユニット（Ｘ）１５は、パソコン３内のハードディスク１９に、音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎを格納している。また、包括管理ユニット（Ｘ）１５は、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎに対応するコンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎも格納している。コンテンツ鍵Ｋｃは、音楽コンテンツＣに対して一対一の関係となっている。また、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎには、それぞれの識別するためのコンテンツＩＤが付加されている。このコンテンツＩＤを、ＣＩＤ１，ＣＩＤ２，ＣＩＤ３・・・ＣＩＤｎとする。

【００８１】

音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎは、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎにより暗号化され、Ｅ（Ｋｃ１，Ｃ１），Ｅ（Ｋｃ２，Ｃ２），Ｅ（Ｋｃ３，Ｃ３）・・・Ｅ（Ｋｃｎ，Ｃｎ）とされた状態でパソコン３のハードディスク１９内に記録されている。ここで、Ｅ（Ｋ，Ｃ）は、鍵ＫでコンテンツＣを暗号化していることを示す。通常、コンテンツＩＤは、音楽コンテンツＣのヘッダなどに記録されて音楽コンテンツＣとともに暗号化されているか、或いは、ＭＡＣが音楽コンテンツＣに付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。

【００８２】

また、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎは、ストレージ鍵ＫＳにより暗号化され、Ｅ（ＳＫ，Ｋｃ１），Ｅ（ＳＫ，Ｋｃ２），Ｅ（ＳＫ，Ｋ

ｃ３）・・・Ｅ（ＳＫ，Ｋｃｎ）とされた状態でパソコン３のハードディスク１９上に記録されている。このストレージ鍵ＫＳは、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。

【００８３】

以上のように鍵管理が行われる包括管理ユニット（Ｘ）１５では、例えば、音楽コンテンツＣ１の再生を行う場合には、ストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、このコンテンツ鍵Ｋｃ１を用いて、音楽コンテンツＣ１の暗号を解除する。このことにより、包括管理ユニット（Ｘ）１５は、音楽コンテンツＣ１の再生を行うことができる。

【００８４】

また、以上のように鍵管理が行われる包括管理ユニット（Ｘ）１５では、例えば、音楽コンテンツＣ１をハードディスク１９からポータブルデバイス（Ｘ）１０に移動（ＭＯＶＥ）する場合には、ポータブルデバイス（Ｘ）１０との間で相互認証を行い、認証が完了するとストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵Ｋｃ１を暗号化し、暗号化したコンテンツ鍵Ｋｃ１及び暗号化した音楽コンテンツＣ１をポータブルデバイス（Ｘ）１０に転送する。そして、コンテンツ鍵Ｋｃ１と音楽コンテンツＣ１をともにハードディスク１９から消去をする。このことにより、包括管理ユニット（Ｘ）１５は、音楽コンテンツＣ１をポータブルデバイス（Ｘ）１０に移動することができる。

つぎに、ハードディスク１９が破壊した場合など、音楽コンテンツやコンテンツ鍵をハードディスク１９から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

【００８５】

まず、通常時において、包括管理ユニット（Ｘ）１５は、ハードディスク１９内に、暗号化した音楽コンテンツＣ及びコンテンツ鍵Ｋｃのバックアップデータを保存しておく。

【００８６】

また、通常時において、包括管理ユニット（Ｘ）１５は、ＥＭＤサーバ（Ｘ）

７からダウンロードした音楽コンテンツの購入記録と、ハードディスク１９内に記憶している全ての音楽コンテンツのコンテンツＩＤのリストとを、使用ログ情報として管理する。このログ情報は、音楽コンテンツをＥＭＤサーバ（Ｘ）７からダウンロードしたときや、ポータブルデバイス（Ｘ）１０への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。包括管理ユニット（Ｘ）１５は、このログ情報を、定期的、或いは、アクセスした度に、ＥＭＤサーバ（Ｘ）７にアップロードする。

【００８７】

そして、包括管理ユニット（Ｘ）１５のハードディスク１９に格納されている音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合には、以下に示すような処理が行われる。

【００８８】

音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合、包括管理ユニット（Ｘ）１５は、まず、ＥＭＤサーバ（Ｘ）７にアクセスを行って、ユーザ認証を行う。

【００８９】

続いて、ＥＭＤサーバ（Ｘ）７は、認証したユーザのユーザＩＤから、包括管理ユニット（Ｘ）１５の使用ログ情報を参照して、整合検証値ＩＣＶ（Integrity Check Value）を生成する。この整合検証値ＩＣＶは、使用ログ情報に記述されている音楽コンテンツＣのコンテンツＩＤであるＣＩＤと、包括管理ユニット（Ｘ）１５のストレージ鍵ＫＳとに基づき、以下のように生成される。

【００９０】

ＩＣＶ＝Ｈ（ＳＫ，ＣＩＤ１｜｜ＣＩＤ２｜｜・・・｜｜ＣＩＤｎ）

ここで、Ｈ（Ｋ，Ｄａｔａ）は、一方向ハッシュ関数で、鍵Ｋによりその値が変化するものである。

【００９１】

続いて、ＥＭＤサーバ（Ｘ）７は、生成した整合検証値ＩＣＶを、包括管理ユニット（Ｘ）１５に送信する。

【００９２】

続いて、包括管理ユニット（Ｘ）１５は、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていれば、そのバックアップデータをリストアして、音楽コンテンツＣ又はコンテンツ鍵Ｋｃをハードディスク１９内に保存する。また、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていなければ、ＥＭＤサーバ（Ｘ）７から破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを再配信してもらう。このとき、ＥＭＤサーバ（Ｘ）７は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

【００９３】

包括管理ユニット（Ｘ）１５は、以上の処理を行い、破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを復活させる。

【００９４】

そして、包括管理ユニット（Ｘ）１５は、復活された音楽コンテンツＣ又はコンテンツ鍵Ｋｃの再生や制御を行う場合には、上記整合検証値ＩＣＶによりその音楽コンテンツのＣＩＤをチェックするようにする。このように、整合検証値ＩＣＶを用いて復活させた音楽コンテンツＣ又はコンテンツ鍵Ｋｃをチェックすることにより、例えば、ある音楽コンテンツＣｉをポータブルデバイス（Ｘ）１０に移動してハードディスク１９上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツＣｉであるＥ（Ｋｃｉ，Ｃｉ）を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

【００９５】

なお、音楽コンテンツＣ及びコンテンツ鍵Ｋｃではなく、ストレージ鍵ＳＫが破壊されている場合には、包括管理ユニット（Ｘ）１５の再インストールを行う。この場合であっても、ＥＭＤサーバ（Ｘ）７にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすることができる。

【００９６】

このように、音楽コンテンツ配信システム１では、例えば、ハードディスクの

クラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

【００９７】

（４）包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット（Ｘ）１５とポータブルデバイス（Ｘ）１０との間では、ポータブルデバイス（Ｘ）１０の固有のＩＤ及び認証鍵（ＭＧ－ＩＤ／ＩＫ）と、包括管理ユニット（Ｘ）１５の固有のマスター鍵（ＯＭＧ－ＭＫ）とを用いて、相互認証が行われる。

【００９８】

包括管理ユニット（Ｘ）１５とポータブルデバイス（Ｘ）１０との間で、相互認証が行われると、包括管理ユニット（Ｘ）１５からポータブルデバイス（Ｘ）１０へ音楽コンテンツを送信したり、ポータブルデバイス（Ｘ）１０から包括管理ユニット（Ｘ）１５への音楽コンテンツの返却をしたりできるようになる。なお、包括管理ユニット（Ｘ）１５は、パソコン３のハードディスク１９内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス（Ｘ）１０は、内部のメモリカード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット（Ｘ）１５からポータブルデバイス（Ｘ）１０へ音楽コンテンツを送信する場合には、パソコン３のハードディスク１９上の音楽コンテンツが、ポータブルデバイス（Ｘ）１０に装着されたメモリカード上に転送されることとなる。また、ポータブルデバイス（Ｘ）１０から包括管理ユニット（Ｘ）１５へ音楽コンテンツを送信する場合には、ポータブルデバイス（Ｘ）１０に装着されたメモリカード上の音楽コンテンツが、パソコン３のハードディスク１９上に転送されることとなる。

【００９９】

ポータブルデバイス（Ｘ）１０は、ＩＤ情報（ＭＧ－ＩＤ）、複数世代分の認証鍵（ＭＧ－ＩＫ）及び複数世代分のマスター鍵（ＯＭＧ－ＭＫ）を予め保持している。ポータブルデバイス（Ｘ）１０には、外部からこれらの鍵等が供給されない。ポータブルデバイス（Ｘ）１０は、必要に応じて、認証鍵（ＭＧ－ＩＫ）

及びマスター鍵（ＯＭＧ－ＭＫ）の世代を更新する。ポータブルデバイス（Ｘ）１０は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス（Ｘ）１０は、第０世代から第９９世代の１００世代分の認証鍵（ＭＧ－ＩＫ［０－９９］）及びマスター鍵（ＯＭＧ－ＭＫ［０－９９］）を保持しているものとする。なお、第ｉ世代の認証鍵を（ＭＧ－ＩＫ［ｉ］）と示し、第ｉ世代のマスター鍵を（ＯＭＧ－ＭＫ［ｉ］）と示す。

【０１００】

また、包括管理ユニット（Ｘ）１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、オーディオ用コンパクトディスク等からパソコン３内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット（Ｘ）１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、ＥＭＤサーバ（Ｘ）７から音楽コンテンツをダウンロードして、パソコン３内に保存することができる。

【０１０１】

ここで、包括管理ユニット（Ｘ）１５では、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）７からは音楽コンテンツをダウンロードすることができないマスター鍵（ＯＭＧ－ＭＫ）と、コンパクトディスクからもＥＭＤサーバ（Ｘ）７からも音楽コンテンツを転送することができるマスター鍵（ＯＭＧ－ＭＫ）とが異なったものとなっている。以下、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）７からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからもＥＭＤサーバ（Ｘ）７からも音楽コンテンツを転送することができる鍵のことをＥＭＤ鍵ともいう。

【０１０２】

なお、本例では、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）がリッピング専用鍵となっており、第１世代以後のマスター鍵（ＯＭＧ－ＭＫ［１～９９］）がＥＭＤ鍵となっている。

【０１０３】

つぎに、リッピング専用鍵を用いた処理の手順について説明する。

【０１０４】

包括管理ユニット（Ｘ）１５がＣＤ－ＲＯＭからインストールされる場合には、図１８に示すように、包括管理ユニット（Ｘ）１５のインストールソフトウェアが格納されたＣＤ－ＲＯＭ５１とともに、ポータブルデバイス（Ｘ）１０と、フロッピーディスク５２とが例えばセットで販売される。フロッピーディスク５２には、ポータブルデバイス（Ｘ）１０のＩＤ情報（ＭＧ－ＩＤ），第０世代の認証鍵（ＭＧ－ＩＫ［０］），第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）が格納されている。

【０１０５】

続いて、販売されたポータブルデバイス（Ｘ）１０等を使用可能とするには、まず、ＣＤ－ＲＯＭ５１をパソコン３に装着する（ステップＳ１１）。続いて、このＣＤ－ＲＯＭ５１から包括管理ユニット（Ｘ）１５をパソコン３にインストールする（ステップＳ１２）。すると、包括管理ユニット（Ｘ）１５がパソコン３のハードディスク内に格納されることとなる（ステップＳ１３）。続いて、フロッピーディスク５２に格納されているポータブルデバイス（Ｘ）１０のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをパソコン３に保存する（ステップＳ１４）。

【０１０６】

このことによって、包括管理ユニット（Ｘ）１５は、音楽ＣＤ５３等により提供される音楽コンテンツを、パソコン３のハードディスク内に格納することができるようになる（ステップＳ１５）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）７から音楽コンテンツをダウンロードできないようになっている。

【０１０７】

また、ポータブルデバイス（Ｘ）１０は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代

とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）１５と、ポータブルデバイス（Ｘ）１０との相互認証が可能となる。したがって、音楽ＣＤ５３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）１０のメモリーカードに格納することができるようになる（ステップＳ１６）。

【０１０８】

一方、包括管理ユニット（Ｘ）１５がネットワークを介して提供される場合には、図１９に示すように、ポータブルデバイス（Ｘ）１０とともに、インターネット上のＷｅｂ５４のアドレス、ユーザＩＤ及びパスワード等が提供される。

【０１０９】

続いて、販売されたポータブルデバイス（Ｘ）１０等を使用可能とするには、まず、ユーザＩＤ及びパスワードを用いてネットワーク上のＷｅｂ５４にアクセスをする（ステップＳ２１）。続いて、Ｗｅｂ５４は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ２２）。続いて、認証に問題がなければ、Ｗｅｂ５４は、包括管理ユニット（Ｘ）１５のインストールソフトウェアと、ポータブルデバイス（Ｘ）１０のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とを、パソコン３に送信する（ステップＳ２３）。続いて、パソコン３は、包括管理ユニット（Ｘ）１５のインストールソフトウェアを起動して、包括管理ユニット（Ｘ）１５をインストールするとともに、ポータブルデバイス（Ｘ）１０のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをハードディスク１９に保存する（ステップＳ２４）。すると、ハードディスクには、包括管理ユニット（Ｘ）１５が格納されることとなる（ステップＳ２５）。

【０１１０】

このことによって、包括管理ユニット（Ｘ）１５は、音楽ＣＤ５３等により提供される音楽コンテンツを、パソコン３のハードディスク１９内に格納することができるようになる（ステップＳ２６）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）７から音楽コ

ンテンツをダウンロードできないようになっている。

【０１１１】

また、ポータブルデバイス（Ｘ）１０は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）１５と、ポータブルデバイス（Ｘ）１０との相互認証が可能となる。したがって、音楽ＣＤ５３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）１０のメモリカード内に格納することができるようになる（ステップＳ２７）。

【０１１２】

なお、以上の図１８及び図１９に示した方法に限られず、包括管理ユニット（Ｘ）１５及びリッピング専用の第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）をＣＤ－ＲＯＭ５１に格納しておき、ポータブルデバイス（Ｘ）１０との認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ）をネットワークを介して提供しても良い。

【０１１３】

つぎに、リッピング専用鍵をＥＭＤ鍵に鍵に更新して、ＥＭＤサーバ（Ｘ）７からダウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。

【０１１４】

包括管理ユニット（Ｘ）１５は、図１８又は図１９に示した手順により、ＣＤ－ＲＯＭ等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パソコン３内のハードディスク１９にインストールされている。このとき包括管理ユニット（Ｘ）１５は、リッピング専用である第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［０］）とを保持しており、ポータブルデバイス（Ｘ）１０の鍵の世代もデフォルトのままである。

【０１１５】

まず、パソコン３は、図２０に示すように、ユーザＩＤ及びパスワードを用い

てネットワーク上のＷｅｂ５４にアクセスをする（ステップＳ３１）。続いて、Ｗｅｂ５４は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ３２）。続いて、認証に問題がなければ、Ｗｅｂ５４は、パソコン３のＩＤ情報（ＯＭＧ－ＩＤ）を登録し、包括管理ユニット（Ｘ）１５がＥＭＤサーバ（Ｘ）７と接続するための公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＳＫ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を生成する（ステップＳ３３）。続いて、Ｗｅｂ５４は、生成した公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＳＫ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を、パソコン３に送信する（ステップＳ３４）。

【０１１６】

続いて、Ｗｅｂ５４は、ポータブルデバイス（Ｘ）１０のＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）をパソコン３に送信する（ステップＳ３５）。続いて、パソコン３の包括管理ユニット（Ｘ）１５は、受信したＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）に基づき、これらの鍵を第ｉ世代に世代更新する（ステップＳ３６）。続いて、包括管理ユニット（Ｘ）１５は、ポータブルデバイス（Ｘ）１０との間で認証を行う（ステップＳ３７）。ポータブルデバイス（Ｘ）１０は、認証がされると、自己の鍵の世代を第ｉ世代に更新する（ステップＳ３８）。

【０１１７】

このことによって、包括管理ユニット（Ｘ）１５は、音楽ＣＤ５３等により提供される音楽コンテンツを、パソコン３のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）７からダウロードした音楽コンテンツをパソコン３のハードディスク１９に格納することができるようになる（ステップＳ３９）。

【０１１８】

つぎに、ＥＭＤ鍵等の世代更新をする手順について説明する。

【０１１９】

包括管理ユニット（Ｘ）１５は、第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［ｉ］）とを保持

しており、ポータブルデバイス（Ｘ）１０の鍵の世代も第ｉ世代となっている。

【０１２０】

まず、図２１に示すように、パソコン３が何らかの処理のため、Ｗｅｂ５４にアクセスすると、Ｗｅｂ５４は、包括管理ユニット（Ｘ）１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）をパソコン３に送信する（ステップＳ４１）。続いて、パソコン３の包括管理ユニット（Ｘ）１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ４２）。続いて、包括管理ユニット（Ｘ）１５は、ポータブルデバイス（Ｘ）１０と認証を行う（ステップＳ４３）。ポータブルデバイス（Ｘ）１０は、認証がされると、自己の鍵の世代を第ｉ世代から第（ｉ＋ｋ）世代に更新する（ステップＳ４４）。

【０１２１】

また、図２２に示すように、一方、ポータブルデバイス（Ｘ）１０が用いている認証鍵等の世代が第（ｉ＋ｋ）世代となっており、包括管理ユニット（Ｘ）１５が保持している認証鍵等の世代が第ｉ世代となっている場合には、ポータブルデバイス（Ｘ）１０と包括管理ユニット（Ｘ）１５との認証が行われると、認証失敗となる（ステップＳ５１）。認証を失敗すると、包括管理ユニット（Ｘ）１５は、Ｗｅｂ５１に対して、鍵要求を行う（ステップＳ５２）。鍵要求があると、Ｗｅｂ５４は、包括管理ユニット（Ｘ）１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）を送信する（ステップＳ５３）。続いて、包括管理ユニット（Ｘ）１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ５４）。続いて、包括管理ユニット（Ｘ）１５は、ポータブルデバイス（Ｘ）１０と認証を行う（ステップＳ５５）。

【０１２２】

このことによって、包括管理ユニット（Ｘ）１５は、音楽ＣＤ５３等により提供される音楽コンテンツを、パソコン３のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）７からダウロードした音楽コンテンツをパソコン３のハードディスク１９に格納することができるようになる（ステップＳ３

８）。

【０１２３】

以上のように、音楽コンテンツ配信システム１では、包括管理ユニット（Ｘ）１５及びポータブルデバイス（Ｘ）１０が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システム１では、サーバから配信された音楽コンテンツの安全性が高まり、例えば、リッピング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

【０１２４】

また、音楽コンテンツ配信システム１では、包括管理ユニット（Ｘ）１５及びポータブルデバイス（Ｘ）１０が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット（Ｘ）１５は、マスター鍵及び認証鍵がネットワークを介して供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

【０１２５】

【発明の効果】

本発明にかかるコンテンツ提供システム及びコンテンツ提供方法では、再生プログラムが、外部記憶媒体に格納されたコンテンツデータのみを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。再生プログラムが、ネットワークを介して提供されたコンテンツデータを取り扱う場合には、第１の認証鍵及び第１のマスター鍵を用いて、外部記憶媒体に格納されたコンテンツデータの保存及び可搬再生装置との認証を行う。第２の認証鍵及び第２のマスター鍵は、ネットワークを介して再生プログラムに提供され、第１の認証鍵及び第１のマスター鍵と異なる鍵となっている。

【０１２６】

このことにより、本発明では、ネットワークを介して配信されたコンテンツデータの安全性を高めることができる

【図面の簡単な説明】

【図１】

本発明の実施の形態の音楽コンテンツ配信システムのシステム構成図である。

【図２】

統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図である。

【図３】

一般的に用いられる利用条件情報のフォーマットを説明する図である。

【図４】

包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。

【図５】

上記統一利用条件情報のオートマトンファイルの構成を説明する図である。

【図６】

上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。

【図７】

上記オートマトンをｔｕｐｌｅ列で表現した図である。

【図８】

上記オートマトン記述部の構成を説明する図である。

【図９】

上記オートマトン記述部の第１の記述例を示す図である。

【図１０】

上記オートマトン記述部の第２の記述例を示す図である。

【図１１】

上記オートマトン記述部の第３の記述例を示す図である。

【図１２】

上記オートマトン記述部の第４の記述例を示す図である。

【図１３】

上記図９～図１２の記述で用いられているイベントとコマンドとを設定した記述例を示す図である。

【図１４】

上記統一利用条件情報のパラメータファイルの構成を説明する図である。

【図１５】

上記パラメータファイルを更新した場合の構成を説明する図である。

【図１６】

上記パラメータファイルのパラメータ記述部の構成を説明する図である。

【図１７】

上記包括管理ユニットによるコンテンツの管理方法について説明する図である。

【図１８】

包括管理ユニットがＣＤ－ＲＯＭからインストールされる場合の処理手順について説明する図である。

【図１９】

包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。

【図２０】

リッピング鍵からＥＭＤ鍵に更新する更新手順について説明する図である。

【図２１】

ＥＭＤ鍵を更新する手順の第１の例について説明する図である。

【図２２】

ＥＭＤ鍵を更新する手順の第２の例について説明する図である。

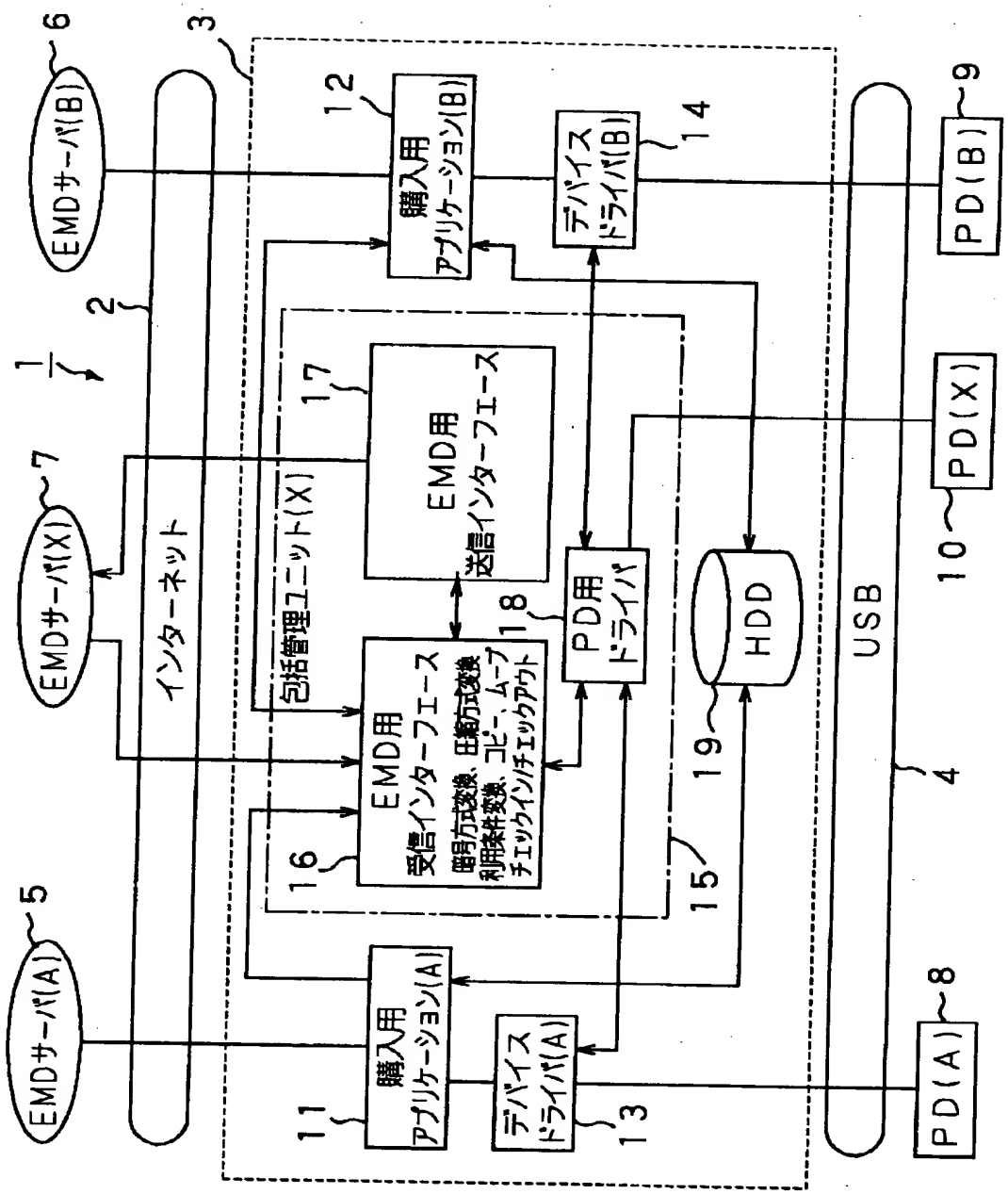
【符号の説明】

１　音楽コンテンツ配信システム、２　ネットワーク、３　パーソナルコンピュータ、４　インターフェース、５，６，７　ＥＭＤサーバ、８，９，１０　ポータブルデバイス、１１，１２　購入用アプリケーション、１３，１４　デバイスドライバ、１５　包括管理ユニット、１６　ＥＭＤ用受信インターフェース、

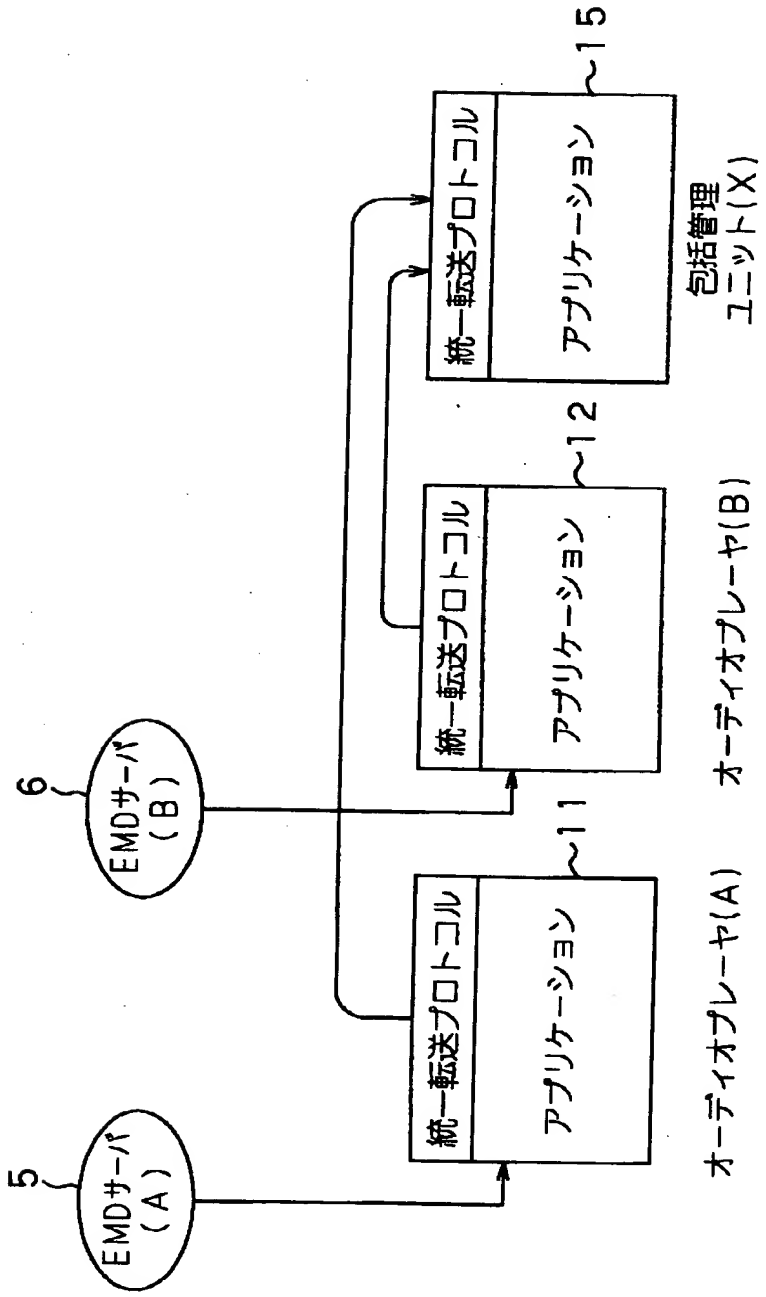
１７　ＥＭＤ用送信インターフェース、１８　ＰＤドライバ、１９　ハードディスク

【書類名】　図面

【図１】


EMDサーバ(B)
6
3
12
購入用
アプリケーション(B)
デバイス
ドライバ(B)
14
PD(B)
9
2
1
17
EMD用
送信インターフェース
包括管理ユニット(X)
EMDサーバ(X)
7
インターネット
PD(X)
10
18
PD用
ドライバ
HDD
USB
EMD用
受信インターフェース
暗号方式変換、圧縮方式変換
利用条件変換、コピー、ムーブ
チェックイン/チェックアウト
16
19
4
15
EMDサーバ(A)
5
購入用
アプリケーション(A)
デバイス
ドライバ(A)
11
13
PD(A)
8

【図２】


EMDサーバ（A）
5
EMDサーバ（B）
6
統一転送プロトコル
アプリケーション
11
オーディオプレーヤ(A)
統一転送プロトコル
アプリケーション
12
オーディオプレーヤ(B)
統一転送プロトコル
アプリケーション
15
包括管理ユニット(X)

【図３】

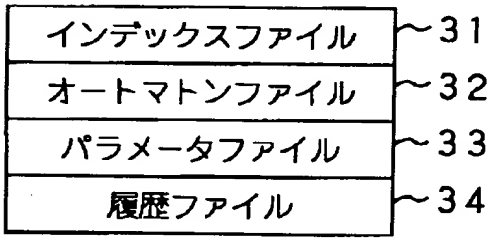
（ａ）

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

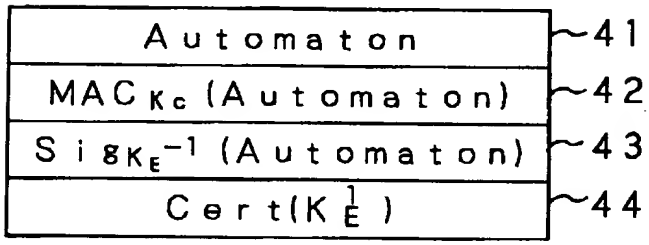
（ｂ）

コンテンツ
利用条件情報

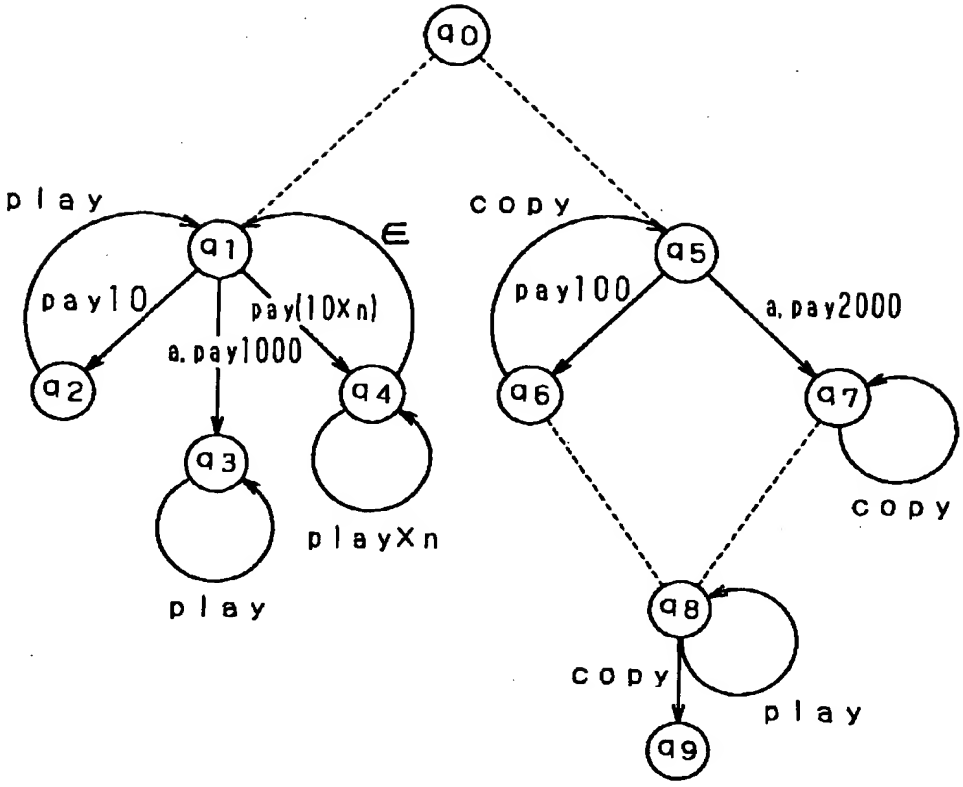
【図４】



【図５】



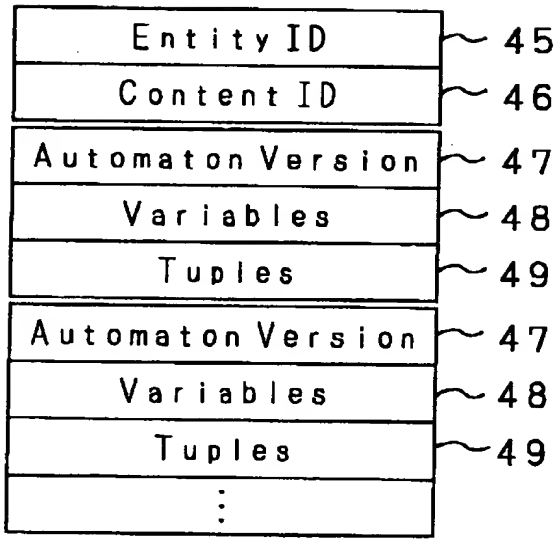
【図６】


q0
play
q1
∈
pay10
pay(10Xn)
a.pay1000
q2
q4
q3
playXn
play
copy
q5
pay100
a.pay2000
q6
q7
copy
q8
copy
play
q9

【図７】

$\langle q_1, pay10, q_2 \rangle$
$\langle q_1, a.pay1000, q_3 \rangle$
$\langle q_1, pay(10 \times n), q_4 \rangle$
$\langle q_2, play, q_1 \rangle$
$\langle q_3, play, q_3 \rangle$
$\langle q_4, play \times n, q_4 \rangle$
$\langle q_4, \epsilon, q_1 \rangle$
$\langle q_5, pay100, q_6 \rangle$
$\langle q_5, a.pay2000, q_7 \rangle$
$\langle q_6, copy, q_5 \rangle$
$\langle q_7, copy, q_7 \rangle$
$\langle q_8, play, q_8 \rangle$
$\langle q_8, copy, q_9 \rangle$

【図８】



【図９】

Content playable from 1999/9/1

```
<automaton>

  <!—This usage rule system has one Right Unit. Initial state is q1 -->
  <initial-right-unit state="q1" />

  <node state="q1">
    <!—If after 1999/9/1, transfer to q2 -->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901" />
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!-- Playable -->
    <rule event="play" next-state="q2" />
  </node>

</automaton>
```

【図１０】

Content playable until 1999/10/31

```
<automaton>

  <!-- This Usage Rule System has one Right Unit. Initial state is q2 -->
  <initial-right-unit state="q2" />

  <node state="q2">
    <!—If after 1999/10/31, transfer to end -->
    <rule event="to" next-state="end">
      <arguments>
        <integer value="time:19991031" />
      </arguments>
    </rule>

    <!-- Playable -->
    <rule event="play" next-state="q2" >
    </rule>
  </node>

  <!—Unusable state-->
  <node state="end" />

</automaton>
```

【図１１】

Content playable less than and/or equal to 16 times

```
<automaton>

  <!—Define valuable counter for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!-- Usage Rule System has one Right Unit. Initial state is q2 -->
  <initial-right-unit state="q1" />

  <node state="q2">
    <rule event="play" next-state="q2" >
      <!—"Count" number of times playable -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!—If this rule is selected , "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

</automaton>
```

【図１２】

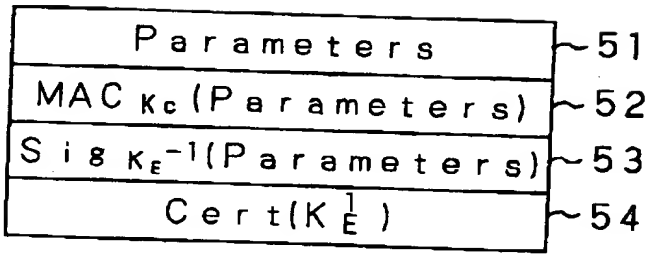
Content playable 16 times from 1999/9/1 to 1999/10/31

```
<automaton>

  <!—Define counter variables for playable numbers. Initial value is 16 -->
  <define-variable name="count" initial-value="16" />

  <!—This Usage Rule System has one Right Unit. Initial state is q1 -->
  <initial-right-unit state="q1" />

  <node state="q1">
    <!—From 1999/9/1 transfer to q2 -->
    <rule event="from" next-state="q2">
      <arguments>
        <integer value="time:19990901" />
      </arguments>
    </rule>
  </node>

  <node state="q2">
    <!—From 1999/10/31, transfer to end -->
    <rule event="to" next-state="end" >
      <arguments>
        <integer value="time:19991031" />
      </arguments>
    </rule>

    <rule event="play" next-state="q2" >
      <!—Playable only for "count" numbers -->
      <arguments>
        <variable name="count" />
        <command name="load" />
      </arguments>
      <!—If this rule is selected, the "count" number decrements by one-->
      <action>
        <variable name="count" />
        <command name="load" />
        <integer value="1" />
        <command name="subtract" />
        <variable name="count" />
        <command name="store" />
      </action>
    </rule>
  </node>

  <!—Unusable state-->
  <node state="end" />

</automaton>
```

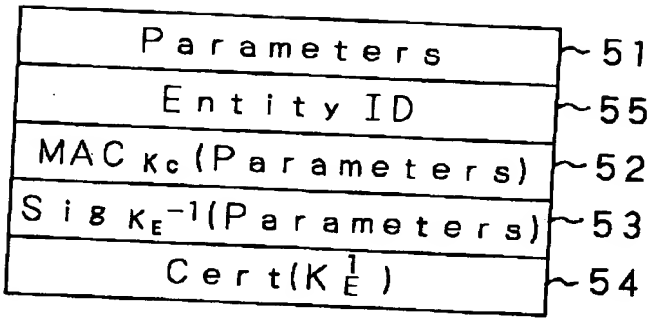
【図１３】

```
<!ENTITY % event "(
    play                |
    copy                |
    pay-for-play        |
    pay-for-copy        |
    pay-for-album-play  |
    pay-for-album-copy  |
    from                |
    to                  |
    null
)">

<!ENTITY % command "(
    drop            |
    dup             |
    swap            |
    add             |
    subtract        |
    multiply        |
    divide          |
    remainder       |
    upper           |
    lower           |
    equal           |
    less            |
    greater         |
    less-equal      |
    greater-equal   |
    and             |
    or              |
    not             |
    bit-and         |
    bit-or          |
    bit-xor         |
    bit-not
)">
```

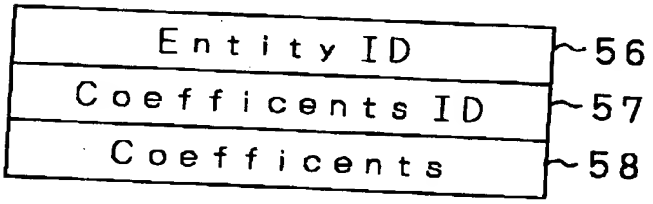
【図１４】



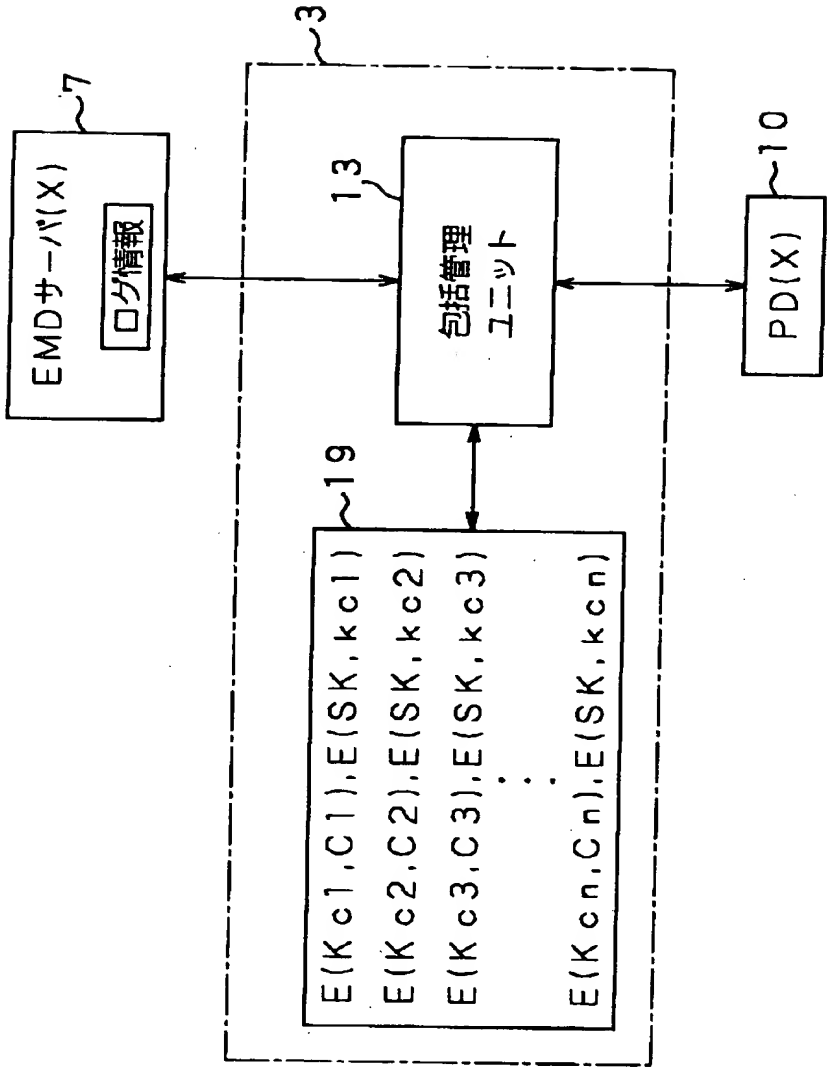
【図１５】


Parameters
51
Entity ID
55
MAC Kc(Parameters)
52
Sig KE-1(Parameters)
53
Cert(KE1)
54

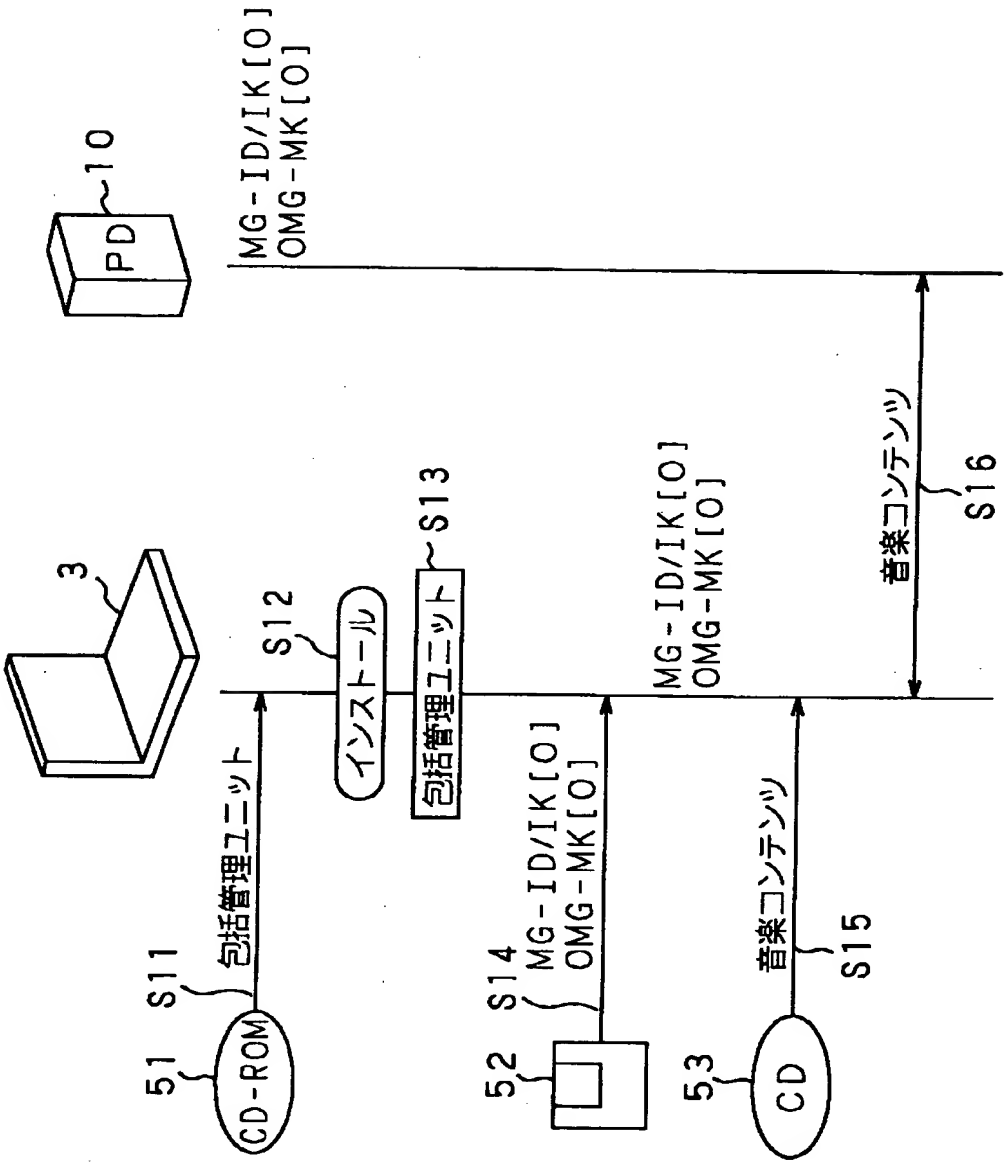
【図１６】


Entity ID
56
Coefficents ID
57
Coefficents
58

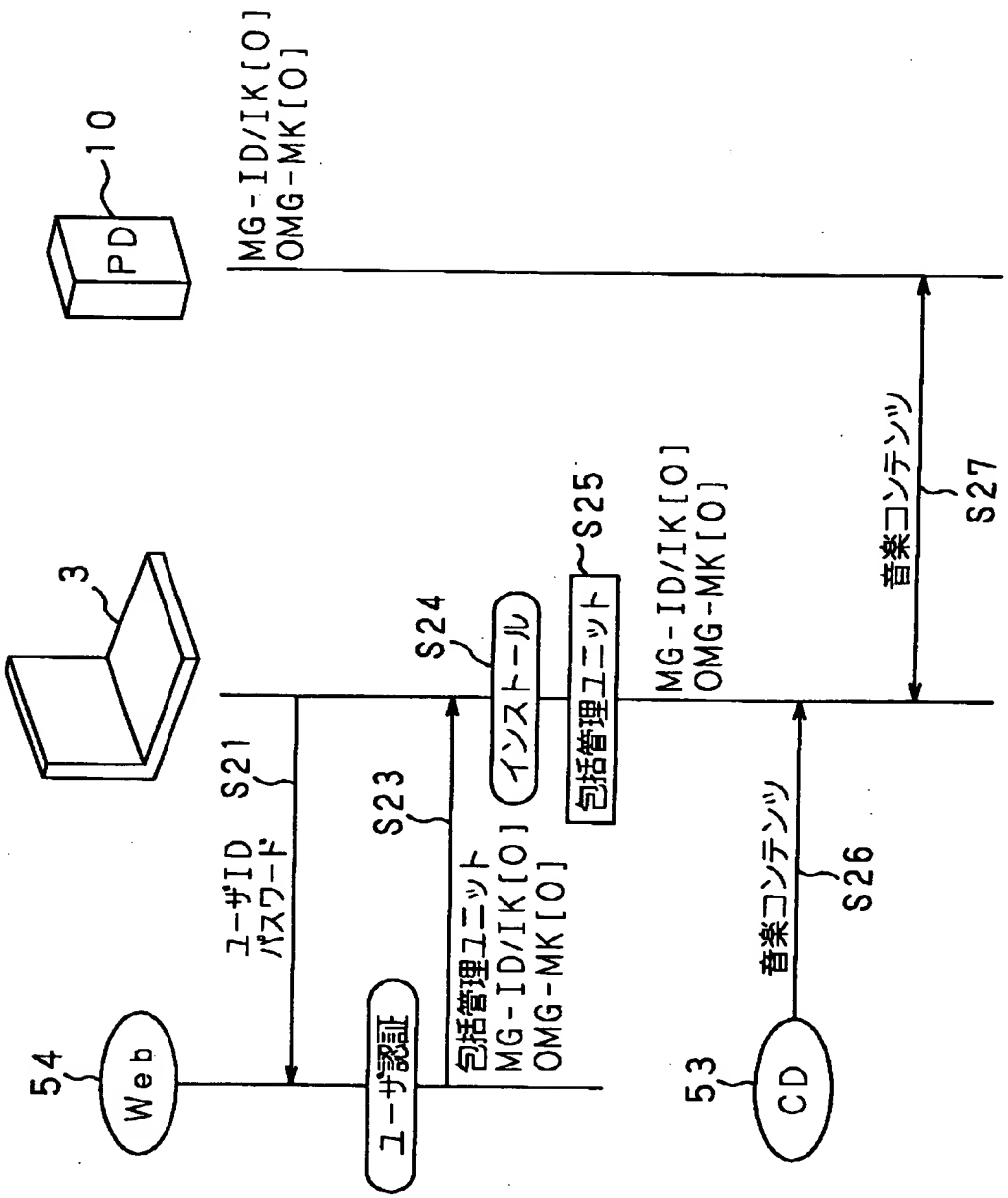
【図１７】


3
7
EMDサーバ(X)
ログ情報
13
包括管理
ユニット
10
PD(X)
19
E(Kc1,C1),E(SK,kc1)
E(Kc2,C2),E(SK,kc2)
E(Kc3,C3),E(SK,kc3)
E(Kcn,Cn),E(SK,kcn)

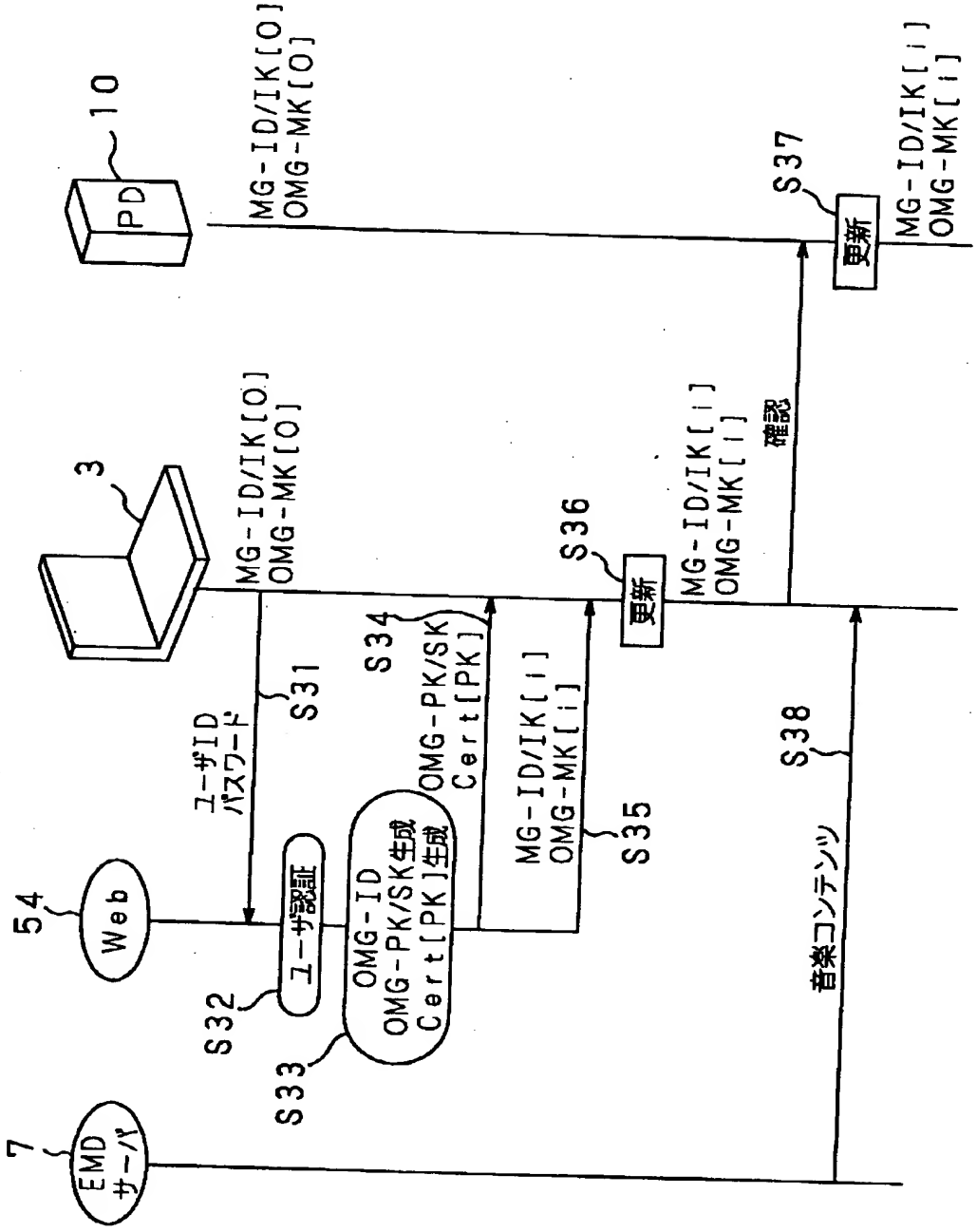
【図１８】


PD
10
MG-ID/IK[O]
OMG-MK[O]
3
S12
インストール
S13
包括管理ユニット
MG-ID/IK[O]
OMG-MK[O]
音楽コンテンツ
S16
S11
包括管理ユニット
51
CD-ROM
S14
MG-ID/IK[O]
OMG-MK[O]
52
音楽コンテンツ
S15
53
CD

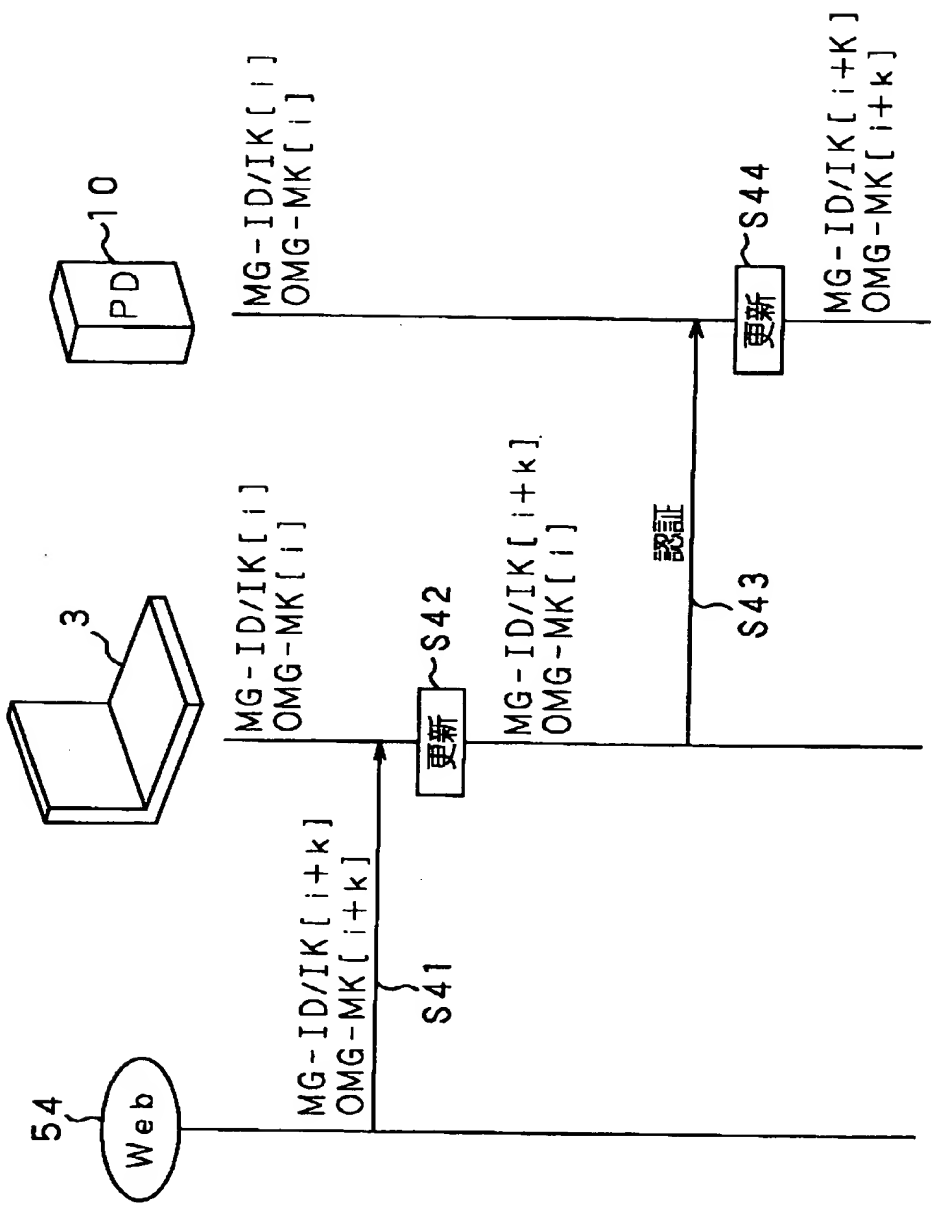
【図１９】


10
PD
MG-ID/IK[O]
OMG-MK[O]
3
S21
ユーザID
パスワード
S23
包括管理ユニット
MG-ID/IK[O]
OMG-MK[O]
S24
インストール
S25
包括管理ユニット
MG-ID/IK[O]
OMG-MK[O]
音楽コンテンツ
S27
54
Web
ユーザ認証
53
CD
音楽コンテンツ
S26

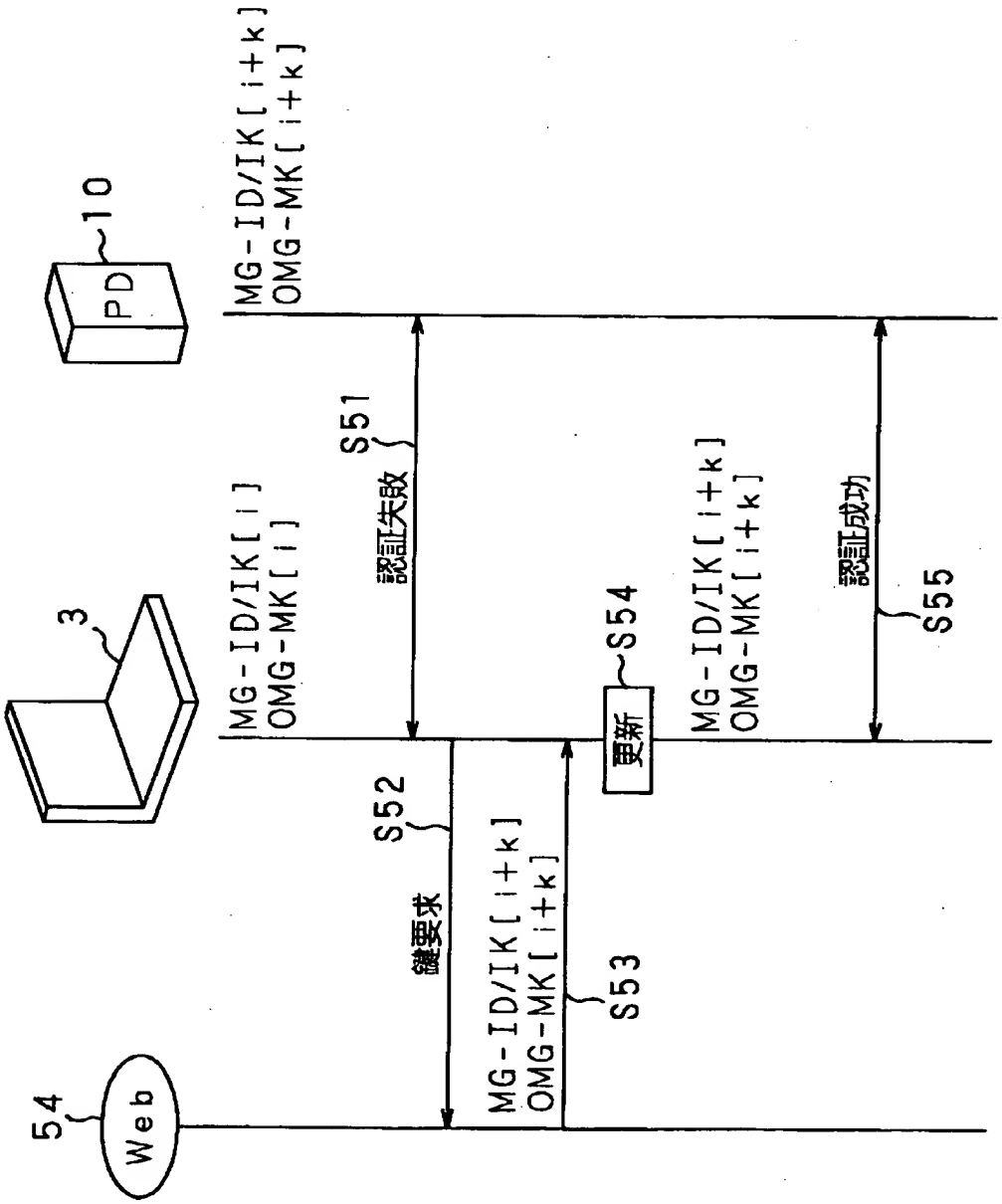
【図２０】


10
PD
MG-ID/IK[O]
OMG-MK[O]
S37
更新
MG-ID/IK[i]
OMG-MK[i]
3
MG-ID/IK[O]
OMG-MK[O]
S36
更新
MG-ID/IK[i]
OMG-MK[i]
確認
S34
OMG-PK/SK
Cert[PK]
S31
ユーザID
パスワード
MG-ID/IK[i]
OMG-MK[i]
S35
S38
音楽コンテンツ
54
Web
ユーザ認証
OMG-ID
OMG-PK/SK生成
Cert[PK]生成
S32
S33
7
EMD
サーバ

【図２１】


10
PD
MG-ID/IK[i]
OMG-MK[i]
S44
更新
MG-ID/IK[i+K]
OMG-MK[i+k]
3
MG-ID/IK[i]
OMG-MK[i]
S42
更新
MG-ID/IK[i+k]
OMG-MK[i]
認証
S43
54
Web
MG-ID/IK[i+k]
OMG-MK[i+k]
S41

【図２２】


10
PD
MG-ID/IK[i+k]
OMG-MK[i+k]
S51
認証失敗
3
MG-ID/IK[i]
OMG-MK[i]
S54
更新
MG-ID/IK[i+k]
OMG-MK[i+k]
認証成功
S55
S52
鍵要求
MG-ID/IK[i+k]
OMG-MK[i+k]
S53
54
Web

【書類名】　要約書

【要約】

【課題】　ネットワークを介して配信されたコンテンツデータの安全性を高める。

【解決手段】　再生プログラムは、ＰＣ上にインストールされた後に、ＣＤのリッピング用の鍵が例えばＦＤから提供される。このＣＤのリッピング用の鍵では、ＣＤ内の音楽コンテンツをＰＤにコピーはできるが、ＥＭＤサーバから音楽コンテンツをダウンロードしてＰＤにコピーすることはできない。再生プログラムは、ＥＭＤサーバから配信された音楽コンテンツをＰＤに保存する場合には、リッピング用の鍵とは異なるＥＭＤ用の鍵をネットワークを介して取得したのちに行う。

【選択図】　図２０

出証特２０００－３０７５３４７

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社